Fraud and Identity Theft

What is Fraud?
Fraud is the crime of deceiving someone to gain money or personal advantage. There are basically two categories of fraud: ones that involve you directly, and ones that gain your personal information without your knowledge.

What is Identity Theft?
Identity Theft occurs when someone uses your personal information without your knowledge or consent, to commit a crime, such as fraud, theft or forgery. Identity thieves and fraudsters seek your financial information (credit card and debit card numbers and PINs, banking information), and your personal identifying information (Social Insurance Numbers, Driver Licence numbers, and other things unique to you).

Who is a Target?
Unfortunately, everyone is a potential target of identity theft. The fact that you 'don't have any money' and have 'maxed out your credit cards' does not prevent you from being a victim.
Examples of how personal information is stolen:

- Stealing a wallet or purse.
- Mail theft of bank and credit card statements and unsolicited credit offers.
- Dumpster diving by rummaging through trash or recycle bins for personal information.
- Changing your mailing address on accounts or by completing a change of address form to divert your mail without your authorization.
- Shoulder surfing at debit machines or using hidden devices to obtain your card number and PIN.
- Skimming (making a fraudulent swipe) of your credit and debit cards while your card transaction is processed.
- Obtaining your personal information from 'inside sources' through theft, bribing or conning information from employees, also known as social engineering.
- Using a scam by posing as a legitimate businessperson or government official to obtain your personal information.

By using some best practices and managing your personal information carefully and sensibly, you can guard against identity theft.

Safeguard your Personal Information:

- When you provide personal information, ask how it will be used, why it is needed, who will be sharing it and how it will be safeguarded. Only give your phone number and email address when needed. (A retail store does not need your phone number unless you want them to contact you.)
- Be aware of who is around when using credit, debit or bank machines and cover the keypad with your other hand while entering your PIN.
- Do not leave receipts at bank machines, businesses, and gas pumps or in trash cans.
- Shred receipts, credit card offers, bank statements, credit card blank cheques (provided by the credit card company), returned cheques, and other sensitive information.
- Shred or destroy unsolicited preapproved credit card or loan applications that come in the mail – they can be used to get credit in your name and with a different address.
- When you order new cheques, pick them up at the bank, and never leave cheques in your vehicle.
- Disclose your Social Insurance Number (SIN) only when it is absolutely necessary and don't carry your card with you.

Guard Your Credit Cards:

- Sign all credit or debit cards as soon as you receive them. Destroy the old ones.
- Never provide your credit/debit cards and Personal Identification Number (PIN) to anyone.

- Don't give your credit card number over the telephone or on a voice mailbox, or by fax or email unless you initiated the transaction, and you know and trust the person/company with whom you are dealing.
- Report any discrepancies or unusual activity on monthly statements immediately.
- Change your card Personal Identification Numbers (PINs) if you have concerns.
- Keep a hidden list of credit and other financial cards you use regularly with account numbers, expiration dates and telephone numbers.
- Do not carry extra credit cards, your Social Insurance Card (SIN), birth certificate or passport unless you need to use them, and put them away safely after use. Cancel cards you do not use.
- Immediately report lost or stolen credit or debit cards.
- Memorize your passwords and Personal Identification Numbers (PINs). If you must write them down, keep this information away from your wallet, and don't write the card number with the PIN.
- Request a copy of your credit report annually from Equifax or TransUnion:
  Equifax - www.consumer.equifax.ca/home/en_ca Telephone: 1-800-465-7166
  TransUnion - www.transunion.ca Telephone: 1-866-525-0262

Protect Your Computer and Mobile Devices:

- Take advantage of technologies that enhance your security and privacy; install a firewall, anti-virus and anti-spyware programs. Ensure system updates are current.
- Do not buy unsolicited anti-virus software that is offered to you on your computer – it is an expensive scam.
- Create long difficult passwords using upper and lowercase letters, numbers and symbols.
- Create an 'extra' email address that you can use at sites that require registration.
- Do not reply to spam or phishing (fake) emails that ask for banking or personal information – Delete them.
- For legitimate online transactions, look for http**s**://, or a closed lock or unbroken key icon in the bottom bar of the computer screen.
- When disposing hard drives, use "overwrite" software or destroy the drive; information that has only been deleted may still be accessible.

If You are a Victim of Identity Theft

- Report the crime to the police immediately. Ask for a copy of the police report so that you can provide proof of the theft to the organizations that you will have to contact later.
- Cancel your credit and debit cards and have new ones issued with new PINs. Close your bank accounts and open new ones. Ask the bank not to cross-reference your new account and cards with the old ones.
- Document the steps you take and the expenses you incur to clear your name and re-establish your credit.
- Have your credit report annotated to document the identity theft. Do a follow-up check three and six months after the theft to ensure that someone has not tried to use your identity again.
- Contact Canada Post if you suspect that someone is diverting your mail.
- Advise your telephone, cable and utilities that someone using your name could try to open new accounts fraudulently.
- Report the crime to the Canadian Anti-Fraud Centre at 1-888-495-8501 and www.antifraudcentre.ca

For more information about Security Awareness:

Information Security Branch Awareness website – www.cio.gov.bc.ca/cio/securityawareness.page

Canadian Anti-Fraud Call Centre - www.antifraudcentre.ca Report fraud – 1-888-495-8501

Public Safety Canada - www.publicsafety.gc.ca/index-eng.aspx